ACCEPTED REVISED PAPER

Protecting Consumer Privacy and Data Security: Regulatory Challenges and Potential Future Directions

Stephen Corones* and Juliet Davis**

This article considers the regulatory problem of online tracking behaviour, lack of consent to data collection, and the security of data collected with or without consent. Since the mid-1990s the US Federal Trade Commission has been using its power under the US consumer protection regime to regulate these problems. The Australian Competition and Consumer Commission (ACCC), on the other hand, has yet to bring civil or criminal proceedings for online privacy or data security breaches, which indicates a reluctance to employ the Australian Consumer Law (ACL) in this field. Recent legislative action instead points to a greater application of the specifically targeted laws under the Privacy Act, and the powers of the Office of the Australian Information Commissioner (OAIC), to protect consumer privacy and data security. This article contends that while specific legislation setting out, and publicly enforcing, businesses' legal obligations with respect to online privacy and data protection is an appropriate regulatory response, the ACL's broad, general protections and public and/or private enforcement mechanisms also have a role to play in protecting consumer privacy and data security.

I. INTRODUCTION

In the mid-1990s online privacy became a major consumer protection issue in the United States of America as a consequence of the development of the Internet and the online environment.[1] Since that time, the transformation of communications and computer processing power has radically affected global commerce. Ecommerce, and 'apps' now available on smartphones, tablets and other devices, have enabled suppliers of goods and services to collect, store, analyse, and re-sell personal information about consumers' online trading activities. While some of this information is supplied by consumers voluntarily, online behaviour tracking is also occurring without the informed consent of consumers.

A related problem is the security of this personal information and data, including financial information such as credit card details, whether collected with or without consent, from cyberattacks. A cyberattack has been defined as:

> …an attempted or actual incident that either:
> (a) uses computer technology or networks to commit or facilitate the commission of traditional crimes, such as fraud and forgery – for example, identity or data theft (computer assisted); or
> (b) is directed at computers and computer systems or other communication technologies – for example, hacking or denial of services (computer integrity).[2]

*BCom, LLB (UQ), LLM (UCL), PhD (UQ); Adjunct Professor, Faculty of Law, Queensland University of Technology.
**BA, LLB (UQ), MA (Columbia University), MSc (London School of Economics and Political Science).

[1] Timothy J Muris, 'The Federal Trade Commission and the Future Development of US Consumer Protection Policy' Paper presented at the Aspen Summit, Cyberspace and the American Dream, Aspen, Colorado, 19 August 2003, 15-25. Available at: https://www.ftc.gov/public-statements/2003/08/federal-trade-commission-and-future-development-us-consumer-protection. See also Maureen K Ohlhausen and Alexander P Okuliar, 'Competition, Consumer Protection, and the Right [Approach] to Privacy' (2015-2016) 80 *Antitrust Law Journal* 121.

[2] ASIC, 'Cyber Resilience: Health Check' (Report 429, ASIC, 2015) 16 [26].

Due to the ubiquitous nature of online transactions, sensitive personal information including financial records, health information, and even intimate relationship details, as seen in the 2015 hack of the online dating service Ashley Madison, are vulnerable to non-consensual exposure and exploitation. The release of this information may cause significant financial and personal costs to the affected parties. As such, businesses and consumers are increasingly recognising the need for cyber protection of personal information. In 2013, Telstra published its *Cyber Security Report 2014*, its first annual survey aimed at compiling and analysing security event data gathered from Telstra infrastructure and security products.[3] It also contains the result of an online survey of professionals responsible for making IT security decisions within their organisations. According to the report's authors,

> As a sign of growing public interest in digital security, the organisations we surveyed perceived reputational damage (22%) as the greatest business risk they faced due to security breaches, alongside productivity loss (22%) and financial loss (21%). Loss of sensitive data wasn't far behind at 20 %.[4]

In March 2015, the Australian Securities & Investments Commission (ASIC) published a report highlighting the importance of cyber resilience and how the risk of cyberattacks and incidents should be met in order to meet current legal and compliance obligations in relation to the supply of financial products and financial services.[5] However it is submitted that current Australian laws protecting consumer privacy and data security have struggled to keep up with the exponential transformations occurring in the online environment. Additionally, it is argued that the current regulatory regime ignores the emerging popularity of self-enforcement mechanisms such as class actions.[6]

Australia's current regulatory approach to this issue has been the adoption of the *Privacy Act 1988* (Cth), specific legislation setting out specific legal obligations for businesses with respect to online privacy and data protection. The *Privacy Act*, administered by the Office of the Australian Information Commissioner (OAIC) establishes economy wide protections and privacy principles for the handing of personal information. However it does not contain a private enforcement mechanism, preventing victims of online privacy and data breach from directly making a legal claim. In contrast, the *Australian Consumer Law* (ACL) located in Schedule 2 of the *Competition and Consumer Act 2010* (Cth) (CCA), does allow for both public and/or private enforcement action. It contains general prohibitions that regulate misleading conduct (s 18), and unconscionable conduct (s 21) and also contains specific prohibitions regulating false or misleading representations relating to the supply of goods or services in trade or commerce. To date the ACL has not served as the basis for either public or private proceedings against online privacy or data security breaches. However, a parallel piece of consumer legislation in the United States, the *Federal Trade Commission Act* has empowered its regulator, the Federal Trade Commission (FTC) to deal with the issue of consumer privacy and companies' data security practices.[7] By examining the FTC's approach to regulating the misuse of consumer information, this article argues that the Australian consumer protection framework could play a role in providing consumer redress against the misuse of online personal data.

The structure of the article is to consider first, in Part II, the nature of the problem and the need for regulation to protect consumers in relation to consumer privacy and data security. Next, in Part III, the specifically targeted laws under the *Privacy Act 1988* (Cth), and the powers of the Office of the Australian Information Commissioner (OAIC), to protect private data are examined. In Part IV the approach of the FTC in using the consumer protection provisions of the *Federal Trade Commission*

[3] Telstra, 'Cyber Security Report 2014' (Report, Telstra, 2014). Available at: http://www.telstra.com.au/business-enterprise/download/document/telstra-cyber-security-report-2014.pdf
[4] Telstra, above n 3, 30.
[5] ASIC, above n 2.
[6] Morabito, V 'An Empirical Study of Australia's Class Action Regimes' (Report 4, August 2016).
[7] Gina Stevens, 'The Federal Trade Commission's Regulation of Data Security under Its Unfair or Deceptive Acts or Practices (UDAP) Authority' (Research Paper, Congressional Research Services, United States Congress, 2014), 1.

Act as a mechanism for protecting consumer privacy and data security, is considered. In Part V, the scope for adopting a similar approach to privacy and data security breaches relying on the broad, general protections of the ACL or equivalent provisions of the ASIC Act, is discussed. While the general nature of the ACL renders it applicable to a greater number of situations, the importance of maintaining the security of financial services necessitates some discussion of the ASIC Act as well. Part VI considers the public and private enforcement under the ACL to deal with online privacy and data security breaches.

II. ONLINE PRIVACY AND DATA SECURITY: THE NATURE OF THE PROBLEM

In June 2013, the Australian Communications and Media Authority (ACMA) published a report which traced the evolution of the personal data environment, citizens' attitudes to digital data sharing and security, and whether current protection mechanisms were adequate to protect personal data.[8] Amongst the emerging gaps in personal data protection, the ACMA identified '…securing an individual's informed consent to the collection and use of their personal information… in an environment characterised by increasingly frequent, varied and complex transactions in the digital information economy.'[9] It also identified '…concerns about the security, privacy and management of personal information that is stored in cloud services, including services housed in other jurisdictions.'[10]

The free flow of information benefits the economy. Consumers will voluntarily disclose their financial information if this will facilitate a transaction. However, consumers are also concerned that information that has been collected may be misused in ways that cause them financial loss, for example, through the denial of credit based on inaccurate financial information; stolen credit card details; and, in extreme cases, identity theft.[11] Incidents of computer hacking and cybercrime are on the rise. A recent global information security survey found that the total number of cybersecurity incidents detected in 2014 was 42.8 million, an increase of 48% from the previous year,[12] with the global cost of cybercrime reaching $575 billion that year.[13] The pervasive, yet precarious, nature of the online data environment has prompted concerns regarding the misuse of consumer information.

There are a number of different approaches to regulating online privacy and data security. One approach is light-handed self-regulation through so-called 'fair information practices' under which businesses make use of Privacy Statements and Privacy Notices that give consumers the opportunity to opt-out of information sharing. However, this approach can be problematic if consumers do not take the trouble to read and understand the Privacy Notice and fail to opt-out. The failure of these light-handed approaches means that more sophisticated regulatory approaches are needed to fix the problem.

This article examines two distinct forms of regulation which have been applied to the misuse of private information in the online data environment. The first regulatory approach is the implementation of specific legislation which allows for the public regulation of privacy and data security breaches, such as the *Privacy Act 1988* (Cth). The second approach allows for the application of general consumer protection legislation which allows for both public and/or private enforcement

[8] ACMA, 'Privacy and Personal Data, Emerging Issues in Media and Communications' (Occasional Paper 4, ACMA, 2013). 15-16 Available at: http://www.acma.gov.au/~/media/Regulatory%20Frameworks%20and%20International%20Engagement/Information/pdf/Privacy%20and%20digital%20data%20protection%20Occasional%20paper%204.pdf

[9] Ibid 23.

[10] Ibid.

[11] Ibid 15-16.

[12] PricewaterhouseCoopers, 'Managing Cyber Risks in an Interconnected World: Key Findings from the Global State of Information Security Survey 2015' (Report, PricewaterhouseCoopers, 2014) 7.

[13] 'The Terrorist in the Data: How to Balance Security with Privacy after the Paris Attacks', *The Economist*, 28 November- 4 December 2015, 23.

action. Examples of this approach include the US *Federal Trade Commission Act*, and we argue, the ACL and ASIC Act.

So far the authors are not aware of any public or private actions in Australia alleging misleading claims by businesses regarding the extent to which they maintain the privacy, security and confidentiality of users' information. One possible reason for the lack of public and private claims is a lack of consumer knowledge regarding specific data breaches. In the past, businesses that are the subject of a cyberattack have not been obliged to notify the consumers whose personal data has been accessed, so that consumers have been unaware that their privacy and personal data may have been compromised. However this situation is expected to change due to the proposed implementation of a mandatory data breach security regime by way of the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015.*

Given the possible increase in consumer awareness of loss or injury caused by online privacy and data security breaches, we believe that there is potential for a shift in the enforcement of these breaches towards an approach that allows for both public and private enforcement. Regulatory theory asserts that social control is maintained via the interplay of public and private enforcement mechanisms.[14] We consider private enforcement in this context to mean the right of individuals and classes of persons to attempt to obtain a remedy, including compensation in the form of damages, from a Court for injury caused by those infringing the regulatory statute.[15] In contrast, public enforcement refers to a wide range of actions undertaken by a public agency in an enforcement role, including the imposition of fines or injunctions, and the commencement of litigation.[16] While public enforcement mechanisms may be considered to operate in the broader public interest and provide relief for those unable or unwilling to take advantage of private forms of legal remedy, they tend to lend themselves less readily to efficiency and effectiveness.[17] Private rights of action act as a check on the competence, diligence, and honesty of public authorities.[18] Where private enforcement mechanisms operate effectively there will be less need for intervention by public authorities.[19] Additionally, it has been argued that:

> Private actions may have a legitimate role in ensuring that those who harm others by their unlawful conduct should be legally responsible to those so harmed. The obligation to pay damages also serves to punish offenders for unlawful action. If the objectives of compensation and punishment are regarded as independent values which should be reflected in the law, then entitling private litigants to seek damages can further these subsidiary goals…It allows those with a direct sense of grievance a direct opportunity to make enforcement claims in court.[20]

Furthermore, we assert that a move towards both public and private enforcement of online privacy and data security breaches is in line with the steady growth of class actions in Australia facilitated by developments in the legal landscape including the acceptance of litigation funding and the expansion of plaintiff class action legal firms.[21] An examination of over 230 federal data breach lawsuits in the United States between 2000 and 2010 found that 76 percent of lawsuits were filed as class actions, with claims under the FTC Act constituting one of the top twenty most common causes of action

[14] Lennon Chang, Lena Zhong and Peter Grabosky, 'Citizen Co-production of Cyber Security: Self-help, Vigilantes and Cybercrime' (2016) *Regulation and Governance* 2.
[15] Karen Yeung, 'Privatizing Competition Regulation' (1998) 18 *Oxford Journal of Legal Studies* 583.
[16] Ibid.
[17] Ibid 587.
[18] Ibid 590.
[19] Chang, above n 14.
[20] Yeung, above n 15, 589.
[21] Allens Linklaters, *Class actions in Australia* (2015), 1. Available at: https://www.allens.com.au/pubs/pdf/ldr/papldrmay15-01.pdf

identified.[22] As such, we consider that general consumer protection legislation, such as the ACL and ASIC Act, may serve as a useful instrument in the regulation and enforcement of online privacy and data security breaches if found to be applicable. In order to determine this question, we will first examine how specific privacy legislation deals with breaches of online privacy and data security, before considering the application of general consumer protection legislation to these issues in both the United States and Australia.

III SPECIFIC PRIVACY LEGISLATION: *PRIVACY ACT 1988* (Cth)

Currently, in Australia, the *Privacy Act 1988* (Cth), administered by the Office of the Australian Information Commissioner (OAIC), regulates the treatment of 'personal information' by certain government agencies and private entities with over $3 million in turnover. 'Personal information' is defined in the *Privacy Act* to mean 'information or an opinion (including information or an opinion forming part of a database and whether or not recorded in material form) about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion'.[23] Schedule 1 of the *Privacy Act* contains thirteen Australian Privacy Principles (APP) that regulate the treatment of personal information by relevant entities.

In relation to the protection of privacy, APP 11 requires regulated agencies and businesses to take 'such steps as are reasonable in the circumstances' to both 'protect the information from misuse, interference and loss, unauthorised access, modification or disclosure' and 'to destroy the information or to ensure that the information is de-identified' once its retention is no longer necessary.[24] The *Privacy Act* does not provide guidance as to what steps are 'reasonable in the circumstances' however the *Guide to Securing Personal Information* released by the OAIC sets out how the OAIC assesses the reasonableness of steps when investigating possible breaches of the *Privacy Act*.[25] Circumstances that will influence the reasonable steps that should be taken include:

> the nature of [the] entity, the amount and sensitivity of the personal information held, the possible adverse consequences for an individual in the case of a breach, the practical implications of implementing the security measure, including the time and cost involved, [and] whether a security measure is itself privacy invasive.[26]

In a consumer context, personal information about shoppers is collected by supermarkets through their loyalty programs. The OAIC has the power under s 33C(1)(a) of the *Privacy Act* to conduct an assessment (audit) to determine whether a private sector entity is complying with the relevant APP. In July 2016, the OAIC issued its final reports in relation to audits of Flybuys loyalty program conducted by Coles Supermarkets Australia Pty Ltd,[27] and the Woolworths Rewards loyalty program conducted by Woolworths Ltd.[28] The assessments were undertaken to determine whether the loyalty programs managed personal information in an open and transparent way as required by APP 1, and whether they notified individuals of the collection of personal information in accordance with APP 5.

---

[22] Sasha Romanosky, 'Empirical Analysis of Data Breach Litigation' (2014) 11(1) .*Journal of Empirical Legal Studies* 74, 83, 101.

[23] *Privacy Act 1988* (Cth).
[24] Ibid; Australian Privacy Principle (APP) 11.1-11.2.
[25] Margaret Jackson and Gordon Hughes, *Private Life in a Digital World* (Thomson Reuters, 2015), 134-135.
[26] Office of the Australian Information Commissioner, *Guide to Securing Personal Information*, (2015) 12.
[27] Available at: https://www.oaic.gov.au/privacy-law/assessments/loyalty-program-assessment-flybuys-coles
[28] Available at: https://www.oaic.gov.au/privacy-law/assessments/loyalty-program-assessment-woolworths-rewards

In relation to data security, regulated entities are not obliged to disclose a data breach to either the OAIC or to the individuals affected.[29] Instead, the OAIC administers a voluntary scheme for reporting data breaches.[30] However, this voluntary reporting structure seems set to change. The Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (Cth),[31] if passed, would require a regulated entity to notify both the OAIC and affected individuals following a 'serious data breach', which is defined as unauthorised access to, or unauthorised disclosure of, personal and certain other information that '…will result in a real risk of serious harm to any of the individuals to whom the information relates…'[32] 'Harm' for the purposes of this section means physical, psychological, emotional, reputational, economic and financial harm.[33] In determining whether there is a 'real risk of serious harm to an individual', a regulated entity may have regard to a number of relevant matters, including the type and sensitivity of the information, the nature of the harm, whether the information is intelligible to an ordinary person, or could be converted into an intelligible form, the kind of person who could obtain the information, and whether steps could be taken to mitigate the harm.[34]

Failure to notify the OAIC and affected individuals of a serious data breach as soon as practicable will be deemed an interference with an individual's privacy contrary to the *Privacy Act* and will trigger the OAIC's existing powers under the *Privacy Act* to 'investigate…make determinations, seek enforceable undertakings and pursue civil penalties for serious or repeated interferences with privacy.'[35] In addition, the proposed mandatory reporting regime would require an organisation to advise affected individuals of the breach either directly, or where this is not practical, by taking reasonable steps to publicise the prescribed matters, including by publishing a copy of those statements on its website.[36] Such publicity may give rise to individual or representative complaints under ss 36 and 38 of the *Privacy Act*.[37] Section 52(1)(b) of the *Privacy Act* provides that after investigating a complaint made under the *Privacy Act*, the Privacy Commissioner may make a determination that:

> (ii) the respondent must perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant;
> (iii) the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint.

IV PRIVACY AND DATA SECURITY & CONSUMER PROTECTION LAW: USA

A second approach to the regulation of online privacy and data security is to focus on the harm that occurs when information is misused and to impose costs on the companies that misuse consumer information in the form of damages under private enforcement, or penalties under public enforcement. We are not aware of any instances where this approach has been adopted in Australia, therefore we will first consider the experience of the United States, where this approach has been adopted by US Federal Trade Commission. The United States, was described by the Australian Law Reform Commission as being at the 'forefront in the development' of mandatory reporting laws regarding data breaches.[38]

---

[29] Australian Government, *Mandatory Data Breach Notification*, Discussion Paper (2015) 2.
[30] Ibid.
[31] Available at https://www.ag.gov.au/Consultations/Documents/data-breach-notification/Privacy-Amendment-Notification-of-Serious-Data-Breaches-Bill-2015-December-2015-exposure-draft.pdf
[32] Exposure Draft Privacy Amendment (Notification of Serious Data Breaches) Bill (Cth), s 26WB(2)(a).
[33] Ibid s 26WF.
[34] Ibid s 26WB(3).
[35] Explanatory Memorandum, Exposure Draft Privacy Amendment (Notification of Serious Data Breaches) Bill (Cth), 5.
[36] Leif Gamertsfelder, 'Disclosure Laws and Class Actions: An Irresistible Relationship' (2016) 5 *Governance Directions* 278.
[37] Ibid.
[38] Australian Law Reform Commission, 'For Your Information: Australian Privacy Law and Practice' Report 108 (May, 2008), 1668 [51.3] available at http://www.alrc.gov.au/publications/report-108.

A Misleading or Deceptive Acts or Practices

The US Federal Trade Commission is empowered by section 5(a) of the *Federal Trade Commission Act* to 'prevent persons, partnerships, or corporations' from using 'unfair or deceptive acts or practices in or affecting commerce'.[39] The FTC has historically tended to use 'deception' more than 'unfairness' as a basis for its litigation due to the comparative ease in identifying deceptive practices that mislead consumers, rather than those which are unfair.[40]

According to the three-factor test set out in the FTC's 1983 Policy Statement on Deception, an act or practice is deceptive if it involves:
(1) 'a representation, omission, or practice that is likely to mislead the consumer';
(2) 'a consumer acting reasonably under the circumstances'; and
(3) the representation, omission, or practice is material to the consumer's choice of or conduct regarding a product or services.[41]

In respect of the first limb of this test, the Commission considers whether the act or practice was 'likely to mislead' the consumer, rather than whether the consumer was actually deceived.[42] Actual harm to a consumer is not necessary; it is sufficient that a company undertook deceptive acts or practices in order for an actionable matter to arise.[43]

The second limb requires the Commission to employ an objective test to consider, from a reasonable consumer's perspective, whether the consumer's reaction to, or interpretation of, the practice was reasonable.[44] This inquiry rests on the specific facts of the matter; and the reasonableness of a consumer's interpretation of an act or omission is presumed if it was the intention of the seller to elicit that interpretation.[45] If a representation by the seller has multiple meanings for a reasonable consumer, the act or omission will still be deemed deceptive provided that one of those meanings is false.[46] In considering the 'reasonableness' of the ordinary consumer's reaction, the Commission will consider a number of factors including 'the clarity of the representation, whether qualifying information is conspicuous, the importance of any omitted information (and whether such information is available elsewhere), and the familiarity of the public with the product or service.'[47] If a particular consumer group is targeted, such as the elderly or children, the Commission will take the perspective 'of an ordinary, reasonable member of that group.'[48] The Commission has emphasised that when assessing this second factor, the entire course of dealing is subject to evaluation and 'when the first contact between a seller and a buyer occurs through a deceptive practice, the law may be violated even if the truth is subsequently made known to the purchaser.'[49] This means that '[w]ritten disclosures or fine print may be insufficient to correct a misleading representation.'[50]

---

[39] Michael D. Scott, 'The FTC, The Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?' (2008) 60(1) *Administrative Law Review* 129.
[40] G.S. Hans, 'Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for a New Era' (2012) 19 *Michigan Telecommunications & Technology Law Review* 171.
[41] Federal Trade Commission, FTC Policy Statement on Deception (14 October 1983) <https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception>
[42] Yan Fang, 'The Death of the Privacy Policy: Effective Privacy Disclosures after In re Sears' (2010) 25 *Berkeley Technology Law Journal* 678.
[43] Eisenhauer, M. *The Information Privacy Case Book: A Global Survey of Privacy and Security Enforcement Actions with Recommendations for Reducing Risks* (International Association of Privacy Professionals, 2008) 26.
[44] Fang, above n 42.
[45] Ibid.
[46] Ibid.
[47] Hans, above n 40, 170.
[48] Fang, above n 42.
[49] Federal Trade Commission, above n 41.
[50] Ibid.

The third limb of this test requires the FTC to determine whether the deceptive representation, omission, or practice is 'material'. The FTC considers a misrepresentation or practice to be 'material' if it is 'one which is likely to affect a consumer's choice of or conduct regarding a product'.[51] 'Material' information must be 'important' to consumers and, if omitted or inaccurate, likely to cause injury to consumers.[52] Certain categories of information are considered by the Commission to be 'presumptively material', such as express and implied claims.[53] The Commission has found claims or omissions to be material where they 'significantly involve health, safety, or other areas with which the reasonable consumer would be concerned' or concern 'the purpose, safety, efficacy, or cost, of the product or service.'[54]

The FTC looks to industry standards in order to determine what constitutes appropriate security practices for companies which deal with the personal information of customers and employees.[55] It has stated that 'to the extent that strong privacy codes are developed, the Commission will view adherence to such codes favourably in connection with its law enforcement work'.[56] A number of industry groups, such as the Better Business Bureau, have now developed 'best practice' standards for privacy and data security.[57] In September 2014, the National Institutes of Standard and Technology's 'Framework for Improving Critical Infrastructure Cybersecurity' was endorsed by the Federal Trade Commissioner as 'fully consistent with the FTC's enforcement framework.'[58]

B Misleading or Deceptive Acts or Practices Cases

The FTC's 'theory of deception' includes instances where specific promises to consumers regarding data security and privacy have been broken, as well as a 'general theory of deception' whereby personal consumer information has been obtained or used without adequate disclosure or consent.[59] Some of the FTC's 'broken promises' cases are relatively clear-cut and require minimal interpretation to determine a violation, such as where a company breaches its own privacy policy.[60] Examples of such 'broken promises' include promises to keep information confidential, ensure sufficient security for personal information, keep consumer identities secret, and refrain from releasing confidential information to third parties.[61] FTC deception cases have also concerned misrepresentations as to the intended use of consumers' personal information and the failure to adhere to privacy policies with third parties.[62]

---

[51] Ibid.
[52] Ibid; Fang, above n 42, 679.
[53] Ibid.
[54] Ibid.
[55] Ibid.
[56] Federal Trade Commission, 'Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers' (March 2012) 14. <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>
[57] Kristina Rozan, 'How Do Industry Standards for Data Security Match Up with the FTC's Implied "Reasonable" Standards—And What Might This Mean for Liability Avoidance?' (2014) *The Privacy Advisor* <https://iapp.org/news/a/how-do-industry-standards-for-data-security-match-up-with-the-ftcs-implied-reasonable-standards-and-what-might-this-mean-for-liability-avoidance>
[58] Ibid.
[59] Daniel J. Solove and Woodrow Hartzog, 'The FTC and the New Common Law of Privacy' (2014) 114(3) *Columbia Law Review* 628.
[60] Ibid.
[61] Ibid 629.
[62] See for example *FTC v. Geocities*, FTC File No. 9823015, Agreement Containing Consent Order (Aug. 1998) and *FTC v. ReverseAuction.com*, Stipulated Consent Agreement and Final Order, Civil Action No. 000032 (D.D.C. Jan. 2000) (FTC File No. 002-3046) discussed in D. Reed Freeman, Jr and Elisa A. Nemiroff, 'Privacy Law: Where Are We Now and Where Are We Headed in 2002 and Beyond?' (2001-2002) 16 *Antitrust* 26.

Although many of these 'broken promises' concerning privacy are expressly stated in company documents such as privacy statements, the Commission also regulates promises made implicitly by the company.[63] For example, in *In re Google Inc.* the company's failure to respect consumers' existing privacy settings was found by the Commission to be a deceptive act, based on the implicit promise that Google would comply with those settings.[64] A company which makes vague promises as to data security and privacy may also be the subject of a FTC deception action.[65]

Many FTC consent orders have considered what constitutes sufficient disclosure in respect of the collection and use of private consumer information. Although these consent orders only bind the intended parties and do not serve as a legal precedent, they do provide an insight into the expanding nature of FTC disclosure and consent requirements with regards to the collection and use of consumers' personal information.

Requirements for a Privacy Statement

In the 1999 matter of *Geocities, a corporation*, the Commission brought an action against an operator of an online community for making false and misleading representations to its consumers through the use of an inadequate privacy statement which failed to disclose its practice of retaining, marketing, and selling consumers' personal information to third parties.[66] In its decision, the Commission put forward a non-exclusive list of disclosures which should be included in a privacy statement. This list included the information collected, its proposed use, and whether it would be shared with third parties.[67] Additionally, the company was to disclose the means by which a consumer could access and remove such information from the company's databases, as well as the process for deleting 'personal identifying data' from the company's database and any limitations to such a deletion process.[68]

The Commission also required that adequate notice as to the company's data security policy appear on the website's home page and every data-collection location.[69] On the home page, there was required to be a 'clear and prominent hyperlink or button labelled **PRIVACY NOTICE**…which directly links to the privacy notice screen(s).'[70] The necessary disclosures had to be displayed 'clearly and prominently' within the privacy statement and there had to be a button for the consumer to press in order to make the privacy notice screen disappear. Additionally, a 'clear and prominent hyperlink' was required at every location where personal identifying data was to be collected which linked directly to the privacy notice screen and was to be accompanied by the following statement, written in bold: '**NOTICE: We collect personal information on this site. To learn more about how we use your information click here**.'[71]

Ongoing Disclosure

The matter of *Sears Holdings Management Corporations*, settled in 2009, demonstrates the FTC's commitment to raising consumer awareness about deceptive data collection.[72] The Commission alleged that Sears created an online service for consumers which required the downloading of a

[63] Solove and Hartzog, above n 59, 629.
[64] Ibid.
[65] Ibid 636.
[66] Courtney J. Merrill, 'Online Privacy Statements' (2000) 41 *New Hampshire Bar Journal* 30.
[67] *In the Matter of GeoCities, a corporation*, FTC File No. 9823015, Decision and Order (Feb. 1999) <https://www.ftc.gov/sites/default/files/documents/cases/1999/02/9823015.do_.htm>
[68] Ibid.
[69] Ibid.
[70] Ibid.
[71] Ibid.
[72] Hans, above n 40, 174.

software application that tracked almost all of the user's online behaviour and internet traffic.[73] This information was then presumably sold to third party data brokers.[74] There were a number of online steps that the consumer needed to take before installing the application, and the software application was not mentioned at every step.[75] An invitation message to those interested in the service stated that research software would track the user's 'online browsing' but did not specify the full extent of the tracking.[76] Sears' 'Privacy Statement and User License Agreement', which consumers had access to later in the joining process, had a more detailed description of the online and offline information gathered but this information was hidden deep in the 75th line of the statement.[77] The scope of the tracking was also not stated in detail at the installation stage. The fact that the application was running was not made obvious to consumers as there was no icon visible on the user's desktop or systems tray.[78] The Commission alleged that Sears' practices were deceptive under section 5 of the FTC Act as initial communications had failed to adequately disclose the extent of information that the software application would collect when installed, facts that 'would be material to consumers in deciding to install the software'.[79]

The final settlement required that Sears disclose adequate information about the tracking application to the consumer and obtain the consumer's express consent prior to the consumer downloading or installing it. Sears was compelled to disclose all of the kinds of data that the application would record, transmit and monitor, including but not restricted to, whether the data would be gleaned from the consumer's use of specific websites or from their broader internet usage, whether the online information would include data obtained from consumer interactions with third parties in secure sessions, shopping basket transactions, online accounts or application forms and whether the data would encompass private health or financial information.[80] Additionally, Sears was to disclose how the online information would be used by the company and whether it would be shared with a third party.[81] This disclosure was to be made 'clearly and prominently, and prior to the display of, and on a separate screen from, any final "end user license agreement," "privacy policy," "terms of use" page, or similar document.'[82]

Furthermore, the FTC set down requirements to ensure that disclosure was 'clear and prominent' in terms of both presentation and content. For disclosures to be 'clear and prominent' they must be 'unavoidable' and 'of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts with the background on which they appear.'[83] Additionally, the disclosure must be comprehensible, in an 'understandable language and syntax, and with nothing contrary to, inconsistent with, or in mitigation of the disclosures.'[84]

---

[73] *In the matter of Sears Holdings Management, a corporation*; FTC File No. 082 3099, Complaint (June 2009) < https://www.ftc.gov/enforcement/cases-proceedings/082-3099/sears-holdings-management-corporation-corporation-matter>; Hans, above n 40, 174.
[74] Ibid.
[75] *In the matter of Sears Holdings Management, a corporation*; FTC File No. 082 3099, Complaint (June 2009) < https://www.ftc.gov/enforcement/cases-proceedings/082-3099/sears-holdings-management-corporation-corporation-matter>
[76] Ibid.
[77] Hans, above n 40, 174.
[78] *In the matter of Sears Holdings Management, a corporation*; FTC File No. 082 3099, Complaint (June 2009) < https://www.ftc.gov/enforcement/cases-proceedings/082-3099/sears-holdings-management-corporation-corporation-matter>.
[79] Ibid.
[80] *In the matter of Sears Holdings Management, a corporation,* FTC File No. 082 3099, Decision and Order (Sept. 2009) < https://www.ftc.gov/enforcement/cases-proceedings/082-3099/sears-holdings-management-corporation-corporation-matter>
[81] Ibid.
[82] Ibid.
[83] Ibid.
[84] Ibid.

The FTC also made clear that the express consent of the consumer was required for the installation of data tracking software and the collection of information. A recommended means of obtaining this consent was to have the consumer click on a button that was not pre-selected as a default and clearly marked as the means by which the tracking process was initiated.[85]

Information Use in Excess of the Privacy Policy

In 2012, Facebook settled with the FTC with respect to a number of alleged deceptive and unfair acts, including collecting and divulging information to third parties and/or the public which it had represented as being subject to user restrictions, and in one count, overriding users' restrictions retroactively.[86] As part of its settlement with Facebook, the FTC ordered that prior to sharing any private user information with a third party which 'materially' exceeded the privacy settings that were in effect for the user, Facebook would both 'clearly and prominently disclose' the proposed sharing arrangement to the user and obtain the 'affirmative express consent of the user'.[87] Specifically, Facebook was required to disclose to the user the kinds of private information that it intended to share with third parties, the third parties' identities or the specific categories they fitted into, and that the proposed sharing arrangement would exceed the private settings that the user had specified for their account.[88] Furthermore, the disclosure of any proposed sharing arrangements was required to be 'separate and apart from any "privacy policy," "data use policy," "statements of rights and responsibilities" page, or other similar document'.[89]

In the matters of *Geocities*, *Sears Holdings* and *Facebook*, the FTC appears to have signalled to businesses that the consumer's informed consent is required prior to any collection or sharing of personal data. As such, companies that use overly complex or vague terms in their disclosure, bury their disclosure in their privacy statement, fail to respect users' choices regarding their privacy settings, or do not provide a means of obtaining express consent, may be exposed to litigation for undertaking deceptive acts or practices.

C Unfair Acts or Practices

Although the FTC has traditionally tended to use 'deception' as the basis of its investigations, it is increasingly using its power to prevent 'unfair acts or practices' as a means of countering online actions that stand outside the specificity of 'deception'. The FTC's test for 'unfairness' was first expressed in the 1980 Policy Statement on Unfairness and later codified into the FTC Act in 1994 as 15 U.S.C. § 45(n).[90]

An act or practice will be considered by the Commission to be unfair if:
(1) 'it causes or is likely to cause substantial injury to consumers
(2) that is not outweighed by countervailing benefits to consumers or to competition and
(3) that cannot be reasonably avoided by consumers'.[91]

The initial factor in the three-limb test of unfairness, the likelihood of substantial injury, should be given the most weight of all the limbs.[92] In order to meet this test, the injury must be substantial; the

[85] Ibid.
[86] *In the Matter of Facebook Inc, a corporation*, FTC File No. 092 3184, Complaint (Aug. 2012) <https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf>
[87] Ibid.
[88] Ibid.
[89] Ibid.
[90] *FTC v. Wyndham Worldwide Corp. et al*, No. 14-3514 (3rd Cir. August 24, 2015) (Opinion).
[91] Fang, above n 42, 676.
[92] Ibid 677.

FTC 'is not concerned with trivial or merely speculative harms'.[93] This factor will typically be satisfied by financial harm, or an unnecessary risk to health or safety, however it may be sufficient to show that a large number of consumers each suffered a small amount of harm.[94] Emotional harm, and other forms of 'subjective' harm, will not ordinarily be considered a 'substantial injury' which will render a practice unfair.[95] For example, the Commission does not purport to ban certain advertisements on the basis that their content may offend some viewers.[96]

The second limb of the unfairness test requires that 'the injury must not be outweighed by any offsetting consumer or competitive benefits that the sales practice also produces'.[97] The Commission recognises that the provision or omission of product information involves balancing the costs and benefits to sellers and consumers. For example, a seller's decision to limit the amount of technical information that they provide to the consumer may reduce the consumer's ability to make an informed purchase, however it also lessens the price of the product.[98] The Commission also has regard to 'the costs to the parties directly before the agency, but also the burdens on society in general in the form of increased paperwork, increased regulatory burdens on the flow of information, reduced incentives to innovation and capital formation, and similar matters.'[99]

Thirdly, the unfairness test requires that the injury could not have been reasonably avoided by consumers. It is the Commission's expectation that the market is self-correcting and that consumers can be relied upon to make their own decisions effectively without regulatory assistance.[100] The Commission will however step in when 'certain types of sales techniques…prevent consumers from effectively making their own decisions.'[101]

§45(n) of the FTC Act provides that '[i]n determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence.'[102] In order to be considered by the FTC, a public policy must be 'clear and well-established.'[103] This means that the policy should not be 'ascertained from the general sense of the national values', but rather stated in 'formal sources such as statutes, judicial decisions, or the Constitution as interpreted by the Courts.'[104] Additionally, the public policy must be widespread; it is insufficient if the established source is limited to a single Court or state decision.[105] The existence of such statutes, cases, or other policies may either support the FTC's view that an act or practice is unfair, or affirmatively allow the action, prompting the Commission to reconsider its preliminary assessment. It is important to note the qualification contained in §45(n) that '[s]uch public policy considerations may not serve as a primary basis for such determination.'[106]

The FTC has historically been rather restrained in pleading 'unfairness', however the use of this pleading is slowly increasing.[107] The FTC has stated that unfairness actions are 'brought, not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller

[93] Federal Trade Commission, FTC Policy Statement on Unfairness (17 December 1980) <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness>
[94] Fang, above n 42, 677.
[95] Federal Trade Commission, above n 93.
[96] Ibid.
[97] Ibid.
[98] Ibid.
[99] Ibid.
[100] Ibid.
[101] Ibid.
[102] 15 U.S.C §45(n).
[103] Federal Trade Commission, above n 93.
[104] Ibid.
[105] Ibid.
[106] 15 U.S.C §45(n).
[107] Solove and Hartzog, above n 59, 638.

behaviour that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decision-making.'[108] A review of the FTC's actions reveals distinct forms of behaviour which constitute unfair trade practices: data collection and use which is deceitful and improper, unfair information security design and practices, and retroactive changes to privacy policies.[109]

The FTC has stated that in the context of data security practices, 'the FTC conducts its investigations with a focus on reasonableness- a company's data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities.'[110] Furthermore, the Commission has emphasised that 'it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and that the mere fact that a breach occurred does not mean that a company has violated the law.'[111]

The FTC has emphasised that in order for a company to have a reasonable data security program, it should:

> (1) [K]now what consumer information they have and what employees or third parties have access to it;
>
> (2) limit the information they collect and retain based on their legitimate business needs;
>
> (3) protect the information they maintain by assessing risks and implementing protections in certain key areas – physical security, electronic security, employee training, and oversight of service provides;
>
> (4) properly dispose of information that they no longer need; and
>
> (5) have a plan in place to respond to security incidents, should they occur.[112]

The majority of the FTC's data security cases have resulted in consent orders, however two companies, LabMD Inc. and Wyndham Worldwide Corporation, together with its subsidiaries, have mounted challenges to the FTC's ability to bring the claims on the basis that 'the FTC lacks authority to regulate companies' data security practices under §5 of the FTC Act, and that the FTC has failed to provide fair notice of what constitutes reasonable data security standards.'[113]

In the matter of *LabMD, Inc*, the FTC considered a company's failure to implement adequate data security practices as constituting an 'unfair practice'.[114] LabMD, a clinical laboratory, was the recipient of sensitive personal information, including consumers' financial and health information.[115] The Commission claimed that failures in LabMD's security system led to the accidental sharing of approximately 9,300 patients' private information on a public file-sharing network.[116] LabMD filed a motion to dismiss the FTC complaint on the basis that it lacked authority to regulate the data security

---

[108] Federal Trade Commission, above n 93.
[109] Solove and Hartzog, above n 59, 640.
[110] Prepared Statement of the Federal Trade Commission, 'Protecting Consumer Information: Can Data Breaches Be Prevented?' before the Committee on Energy and Commerce (5 February 2014), cited in Kathryn F. Russo, 'Regulation of Companies' Data Security Practices Under the FTC Act and California Unfair Competition Law' (2015) 32(5) *The Computer & Internet Lawyer* 15.
[111] Federal Trade Commission, Commission Statement Marking the FTC's 50th Data Security Settlement (31 January 2014) < https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf>
[112] See Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Nov. 2011) cited in Gina Stevens, above n 7, 4.
[113] Russo, above n 110, 15-16.
[114] Ibid 14.
[115] Ibid 18.
[116] Ibid.

procedures of companies under section 5 and that it failed to give adequate notice as to the meaning of 'reasonable data security standards'.[117] The FTC subsequently made an order denying LabMD's motion to dismiss.[118]

On 13 November 2015, Chief Administrative Law Judge Chappell dismissed the FTC's charge of unfair trade practice against LabMD on the basis that the Commission 'failed to prove that the allegedly unreasonable conduct caused or was likely to cause substantial injury to consumers.'[119] In his Initial Decision, Judge Chappell found that the FTC failed to prove that 'the exposure or limited exposure of some LabMD documents in 2008 has caused, or is likely to cause, any substantial consumer injury (whether identity-theft-related harm or otherwise).'[120] Furthermore, the Court held that 'demonstrating actual or likely substantial consumer injury under Section 5(n) [of the FTC Act] requires proof of more than the hypothetical or theoretical harm that has been submitted by the government in this case.'[121] On 24 November 2015, the FTC's complaint council lodged an appeal of Judge Chappell's Initial Decision with the full Federal Trade Commission. Whilst Judge Chappell's decision is a blow to the FTC's pursuit of LabMD, it is important to note for the purpose of this article that the Court's dismissal of the charge of unfair trade practice was founded on findings of fact in this particular matter, rather than a denial of the FTC's authority to regulate companies' data security practices under §5 of the FTC Act. The matter is ongoing.

Wyndham Worldwide Corporation's computer network was the subject of hacker attack on three separate occasions, which led to losses in excess of $10.6 million dollars.[122] The FTC brought an action against Wyndham Worldwide Corporation and a number of its subsidiaries, alleging, amongst other things, that its claim that it protected the personal information of customer by using 'industry standard practices' was untrue and deceptive, and that its failure to maintain a 'reasonable and appropriate data security standards' for the personal information of its consumers violated section 5 of the FTC Act.[123] Specifically, the FTC alleged that WWC had 'unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft' by:

(1) 'fail[ing] to use firewalls';
(2) 'stor[ing] payment card information in clear readable text';
(3) 'fail[ing] to implement adequate information security policies and procedures'
(4) 'fail[ing] to remedy known security vulnerabilities';
(5) 'us[ing] default user IDs and passwords';
(6) 'not requir[ing] the use of complex passwords';
(7) 'fail[ing] to adequately inventory computers';
(8) 'fail[ing] to employ reasonable measures to detect and prevent unauthorized access to computer networks';
(9) 'fail[ing] to following proper incident response procedures';
(10) 'fail[ing] to adequately restrict third-party vendors' access to Wyndham's network'.[124]

Based on the above alleged violations, the FTC requested that the US District Court for the District of New Jersey impose a permanent injunction and other orders as the Court saw fit.[125] WWC filed a

[117] Ibid.
[118] Ibid.
[119] Federal Trade Commission, 'Administrative Law Judge Dismisses FTC Data Security Complaint Against Medical Testing Laboratory LabMD, Inc.' (Media Release, 19 November 2015).
[120] Ibid.
[121] Ibid.
[122] Russo, above n 110, 16.
[123] Ibid; Woodrow Hartzog and Daniel J. Solove, 'The FTC as Data Security Regulator: FTC v. Wyndham and Its Implications' (2014) 13 *Bloomberg BNA Privacy & Security Law Reporter* 623.
[124] Russo, above n 110, 16.
[125] Ibid.

motion to dismiss the FTC's complaint on the basis that § 5 of the FTC Act did not provide the FTC with the authority to regulate unfairness with respect to data security, that the FTC had not provided 'fair notice' as to what it considered to be 'reasonable data security standards', and that the security of card data was not governed by § 5 of the FTC Act. [126]

By denying Wydham's motion to dismiss, the US District Court for the District of New Jersey upheld the FTC's authority to bring an action against deceptive and unfair conduct in the context of data security.[127] Additionally, it confirmed that the FTC had provided fair notice as to what constitutes unfairness with respect to data security practice and was not required to publish regulations before bringing an unfairness claim.[128] WWC immediately filed a motion for interlocutory appeal to the Third Circuit on the questions of whether the FTC had the authority to bring an unfairness claim under § 5 and whether the formal promulgation of regulations was a necessary first step before bringing an unfairness claim.

On August 25, 2015 the Third Circuit dismissed WWC's interlocutory appeal, affirming the District Court's decision that the FTC does have authority to regulate a company's data security procedures by way of section 5 of the FTC Act, also holding that WWC was given fair notice as to the possible application of the Commission's unfairness standard to its data security practices. Further, it held that the FTC adequately alleged that 'substantial injury' to consumers had occurred, as required under section 5.[129] On 9 December 2015, Wyndham announced that it would settle the matter with the FTC, agreeing to set up a 'comprehensive information security program' designed to safeguard the security and integrity of cardholder data.[130]

Clearly, the Commission considers issues of consumer privacy and data security to be within its power to prevent unfair or deceptive acts or practices under section 5 of the FTC Act, a view which at this stage appears to be supported by the Courts. Given the current lack of direct legal avenues for individuals affected by data breaches in Australia, the following section will consider the applicability of a similar consumer protection approach by way of the *Australian Consumer Law*.

V PRIVACY AND DATA SECURITY & CONSUMER PROTECTION LAW: AUSTRALIA

In this Part we will consider how the three general protections in the ACL, in relation to misleading conduct, unconscionable conduct, and unfair terms respectively, can apply to specific situations involving online privacy and data protection.

A Misleading or Deceptive Acts or Practices

This Part examines how well the prohibitions of misleading conduct and unconscionable conduct in the *Australian Consumer Law* capture online privacy and data security breaches that are harmful to consumers. The first general protection contained in s 18(1) of the ACL provides that:

> A person must not, in trade or commerce, engage in conduct that is misleading or deceptive or is likely to mislead of deceive.

This prohibition does not substantively vary from s 52(1) of the *Trade Practices Act 1974* (Cth)

[126] Ibid.
[127] Ibid.
[128] Ibid 17.
[129] Caleb Skeath, 'Third Circuit Upholds FTC's Data Security Authority in FTC v Wyndham' (2015) *The National Law Review* 1.
[130] *Federal Trade Commission v Wyndham Worldwide Corporation, et al*, Civil Action No. 2:13-CV-01887-ES-JAD, Proposed Stipulated Order For Injunction (Dec. 2015) <https://www.ftc.gov/system/files/documents/cases/151209wyndhamstipulated.pdf>

(TPA), and the State and Territory equivalents in their Fair Trading Acts (FTA). The only difference is that s 18 is directed at the conduct of persons generally rather than corporations. If the conduct concerns that of a corporation reliance will generally be placed on the ACL (Cth). If the conduct concerns that of natural persons, reliance will generally be placed on the ACL of the State or Territory in which the conduct occurred.

In *Campomar Sociedad Limitada v Nike International Ltd*, the majority, in a joint judgment stated:

> Where the persons in question are not identified individuals to whom a particular misrepresentation has been made or from whom a relevant fact, circumstance or proposal was withheld, but are members of a class to which the conduct in question was directed in a general sense, it is necessary to isolate by some criterion a representative member of that class. The inquiry thus is to be made with respect to this hypothetical individual why the misconception complained has arisen or is likely to arise if no injunctive relief be granted. In formulating this inquiry, the courts have had regard to what appears to be the outer limits of the purpose and scope of the statutory norm of conduct fixed by s 52.[131] (citations omitted)

Thus, where conduct is directed at the public, the class is first identified. Having identified the class, the effect of the conduct is assessed having regard to the reactions of the 'hypothetical individual' – the ordinary, reasonable member of the class, not those of persons whose reactions are 'extreme or fanciful'.[132]

The concept of 'engaging in conduct' in s 2(2) of the ACL divides conduct into two broad categories: 'doing any act' and 'refusing to do any act'. The statutory language used does not require the making of some representation. As Hayne J observed in *Google Inc v ACCC*, the focus must be on the statutory text which focuses on 'conduct' rather than 'representations'.[133] In many situations the respondent's silence will not occur in isolation. The relevant 'conduct' will consist of the whole factual matrix including actions, representations and omissions (silence) that, viewed as a whole, may be misleading. In cases such as these, the presence of the additional material, when combined with the silent party's failure to disclose, may render its conduct, viewed in its entirety, misleading or deceptive for the purpose of s 18 of the ACL.[134]

Assuming that the definition of 'conduct' in s 2 of the ACL can be satisfied, it is then necessary to consider whether silence at issue in a particular case was misleading. In *Miller & Associates Insurance Broking Pty Ltd v BMW Australia Finance Limited*, different approaches were taken for determining whether the conduct at issue was misleading.[135] One approach was to analyse whether the

---

[131] *Campomar Sociedad Limitada v Nike International Ltd* (2000) 202 CLR 45 at 85 [103] (Gleeson CJ, Gaudron, McHugh, Gummow, Kirby, Hayne and Callinan JJ). See also *Google Inc v ACCC* (2013) 249 CLR 435 at [6]-[9] (French CJ, Crennan and Kiefel JJ); *Astrazeneca Pty Ltd v GlaxoSmithKline Australia Pty Ltd* [2006] ATPR ¶42-106 at [37] (Wilcox, Bennett and Graham JJ); *ACCC v Telstra Corporation Ltd* (2007) ATPR ¶42-203 at [14]-[15] (Gordon J); *Energizer Australia Pty Ltd v Remington Products Australia Pty Ltd* (2008) ATPR ¶42-219 at [16] (Moore J); and *ACCC v Prouds Jewellers Pty Ltd* (2008) ATPR ¶42-217 at [16]-[19] (Moore J).

[132] *Miller & Associates Insurance Broking Pty Ltd v BMW Australia Finance Limited* (2010) 241 CLR 357. See also *Campomar Sociedad Limitada v Nike International Ltd* (2000) 202 CLR 45 at 86-87 [105]; and *Forrest v Australian Securities and Investments Commission* [2012] HCA 39 (2 October 2012) at [49]-[50] (French CJ, Gummow, Hayne and Kiefel JJ).

[133] *Google Inc v Australian Competition and Consumer Commission* (2013) 249 CLR 435 at 465-6 [92]-[96] (citations omitted).

[134] *Noor Al Houda Islamic College Pty Ltd v Bankstown Airport Ltd* (2005) 215 ALR 625; *Wright v Wheeler Grace & Pierucci Pty Ltd* (1988) ATPR ¶40-865 at 49,375-49,376 (French J); affirmed in *Wheeler Grace & Pierucci Pty Ltd v Wright* (1989) 16 IPR 189 ; *Bateman v Slayter* (1987) 71 ALR 553 at 559 (Burchett J).

[135] *Miller & Associates Insurance Broking Pty Ltd v BMW Australia Finance Limited* (2010) 241 CLR 357 at [19]. See Bernard McCabe, 'When Silence Misleads, and When it Doesn't' (2011) 19 *Australian Journal of Competition and Consumer Law* 47, 49-51.

conduct viewed as a whole, conveyed a representation which was misleading. Another approach was to analyse whether the circumstances gave rise to a 'reasonable expectation' that if some relevant fact existed, it would be disclosed to the person who claimed to have been misled.[136]

In addition to the general protection for misleading conduct contained in s 18, the ACL contains specific protections for false or misleading representations in relation to the supply of goods or services in s 29(1). Section 18 of the ACL is a general provision dealing with misleading conduct and only gives rise to civil liability. Section 29(1) is more specific in its terms and gives rise to criminal as well as civil liability. It provides that:

> A person must not, in trade or commerce, in connection with the supply or possible supply of goods or services or in connection with the promotion by any means of the supply or use of goods or services:
>
> (a) make a false or misleading representation that goods are of a particular standard, quality, value, grade, composition, style or model or have a particular history or particular previous use; or
> (b) make a false or misleading representation that services are of a particular standard, quality, value or grade; or
> …
> (g) make a false or misleading representation that goods or services have sponsorship, approval, performance characteristics, accessories, uses or benefits;

The equivalent provision of the TPA was s 53(c) and the jurisprudence in relation to s 53(c) will apply in relation to s 29(1)(g).[137] As for s 18 of the ACL, a representation can be made to identified individuals, or to members of a class or section of the public. Section 29 of the ACL applies to false *or* misleading representations. The term "false" in relation to s 53 of the TPA was construed to mean "contrary to fact", and did not depend on the knowledge of the person making the representation. In *Given v Holland (Holdings) Pty Ltd*, the representation consisted of an odometer reading of a motor vehicle displayed for sale in the defendant's second-hand car yard. The odometer showed a mileage of 23,700 when, in fact, the vehicle had travelled approximately 69,012 miles.

Franki J held in relation to s 53(a):

> I am satisfied that, if a representation is in fact not correct, it comes within the words of the section, even if it is not false to the knowledge of the person making the representation, and even if the person making the representation is a servant of the company of insufficient significance in the company for his knowledge, according to the ordinary principles of the Common Law, to be deemed to be the knowledge of the company.[138]

---

[136] The genesis of the "reasonable expectation" approach is to be found in the judgment of Gummow J in *Demagogue Pty Ltd v Ramensky* (1992) 39 FCR 31 at 41.

[137] See *ACCC v Excite Mobile Pty Ltd* (2013) ATPR ¶42-437 (Mansfield J); *ACCC v Harvey Norman Holdings Limited* (2011) ATPR ¶42-384 (Collier J); *ACCC v GM Holden Ltd* [2008] FCA 1428 (18 September 2008); *CPA Australia Ltd v Dunn* (2007) ATPR ¶42-205 (Weinberg J); *Osgaig Pty Ltd v Ajisen (Melbourne)Pty Ltd* (2004) ATPR ¶42-036 (Weinberg J); *ACCC v Chen* (2003) ATPR ¶41-948 (Sackville J); *ACCC v Wizard Mortgage Corp Ltd* (2002) ATPR ¶41-903 (Merkel J); *Mark Foys Pty Ltd v TVSN (Pacific) Ltd* (2001) ATPR ¶41-795 (Beaumont, Tamberlin and Emmett JJ); *ACCC v Giraffe World Australia Pty Ltd (No 2)* (1999) ATPR ¶41-718 (Lindgren J); and *Glendale Chemical Products Pty Ltd v ACCC* (1999) ATPR ¶41-672 (Wilcox, Tamberlin and Sackville JJ).

[138] *Given v C V Holland (Holdings) Pty Ltd* (1977) ATPR ¶40-029 at 17,386. Franki J placed reliance on the High Court's interpretation of "false" as meaning "contrary to fact" in s 234(d) of the *Customs Act 1901* (Cth) in *Sternberg v The Queen* (1953) 8 CLR 646 and *Davidson v Watson* (1953) 28 ALJ 63 at 64.

The test for determining whether representations in relation to goods or services are "misleading" for the purposes of s 29(1) is the same as that adopted for determining whether conduct is misleading for the purposes of s 18(1) of the ACL.

Whether a representation directed at identified persons is misleading will be dictated by the circumstances of each particular case, including the state of knowledge of the person to whom the representation is directed. The test is: would a reasonable person in the position of the representee, taking into account what they knew, have been misled by the representation.[139]

Part II, Div 2, Subdiv D of the ASIC Act mirrors the ACL. It contains a broad general protection (s 12DA) against misleading or deceptive conduct in relation to financial services or financial products, the equivalent of s 18 of the ACL, and then contains more specific protections – first, the making of specific false or misleading representations in relation to financial services.[140] Section 12CC of the ASIC Act mirrors s 21 of the ACL and regulates unconscionable conduct in relation to the provision of financial products and financial services.

B Misleading or Deceptive Acts or Practices Cases

Misleading Statements concerning Data Protection Measures

Where a corporation mispresents to consumers its data protection measures, that is plainly misleading or deceptive conduct and will contravene ss 18, 29(1)(a),(b) and/or 29(1)(g). It will constitute false or misleading representation that the goods or services are of a particular standard or quality and had certain performance characteristics. Misleading statements concerning data protection measures would include:

- falsely claiming to keep consumers' information confidential or to keep consumer identities secret;
- falsely claiming that consumers' information is securely encrypted and stored;
- falsely claiming not to release confidential information to third parties.; and
- falsely claiming that a corporation's data security practices exceed or surpass industry security standards.

Representations Regarding the Use of Industry Standard Practices

The protection of software and hardware from unauthorised access or disclosure generally requires businesses to ensure that sensitive information is encrypted during transmission and storage. In some cases representations concerning data security claims are made by representors who know that the representations cannot be supported, and who also know that the target audience will not be able to check the accuracy of the claim because of the information asymmetry between the maker of the representation and the audience. In cases involving information asymmetry, or where representors hold themselves out as having specialist knowledge or expertise, the Court may find that a reasonable member of the target audience may conclude that the representation conveyed not merely that the maker believed the claim, but also that there were reasonable grounds for that belief, or, in the case of scientific or medical claims, that there was an adequate scientific or medical basis for the claim. If there is no adequate basis to substantiate the claim it will be found to be misleading.

[139] *Butcher v Lachlan Elder Realty Pty Ltd* (2004) 218 CLR 592 at [50].
[140] ASIC Act, s 12DB(1).

In *ACCC v Breast Check Pty Ltd*,[141] Breast Check published promotional pamphlets stating that its thermography devices for conducting breast imaging could be used for assessing whether a customer was at risk from breast cancer and the level of that risk. The ACCC also alleged that Breast Check's claim contained a representation that there was an adequate scientific basis for using the thermography devices as a substitute for mammography. It was held that Breast Check had contravened s 53(c) of the TPA and s 29(1)(g) of the ACL. Barker J found:

> In the context of a representation of a medical nature … it would be entirely reasonable for a consumer to conclude that, where a service of a medical nature is being provided, there would be scientific medical evidence of a sufficient quality to support the use of the equipment used to provide such a service and that the use of breast imaging devices would not be promoted in a way as to be contrary to the state of scientific medical knowledge.[142]

What constitutes an "adequate" basis was considered by Barker J who stated:

> As to the question of the representation conveying that there is an adequate scientific or medical basis, I accept the submission made on behalf of ACCC that the word "adequate" should be taken in the sense by which it is generally understood. In the medical context that is that the service is provided according to evidence based medical knowledge and that there is sufficient support in medical science for the use of the devices for the purposes represented. This is particularly so in the context of assessing whether or not a person may have or be at risk of breast cancer, which is clearly a question of medical science.[143]

Upon examining the above cases, it is submitted that if the facts in *FTC v Wyndham* arose in Australia and false representations were made by a corporation that it protected the personal information of customers by using 'industry standard practices', the conduct would give rise to contraventions of ss 18 and /or 29(1)(g) of the ACL, or ss 12DA and/or 12DB(1) of the ASIC Act.

Obtaining Personal Information without Consent

The FTC's 'theory of deception', applying where personal information is obtained without consent, is potentially important in the Australian context. A corporation that makes promises implicitly and a corporation which makes vague promises as to data security and privacy may also be the subject of a misleading conduct action. Deliberate failure to disclose adequate information about software applications that track consumers' online behaviour and internet traffic is likely to contravene s 18 of the ACL. Silence through inadvertence does not invoke these provisions; the relevant refusing or refraining must be engaged in deliberately.[144] Where a corporation engages in conduct that involves silence, and it is necessary to establish that the corporation deliberately failed to disclose within the definition of conduct in s 2(2)(c) of the ACL, s 139B(1) of the *Competition and Consumer Act 2010* (Cth) must be considered. Section 139B(1) provides that if in a proceeding under the ACL in respect of conduct engaged in by a body corporate, it is necessary to establish the state of mind of the body corporate, it is sufficient to show (a) 'that a director, employee or agent of that body corporate engaged in that conduct within the scope of the actual or apparent authority of the director, employee or agent'; and (b) 'that the director, employee or agent had that state of mind.'

---

[141] *ACCC v Breast Check Pty Ltd* (2014) ATPR ¶42-479.
[142] Ibid at [141].
[143] Ibid at [139]. There is a line of authority that supports this approach. See *Global Sportsman v Mirror Newspapers* (1984) 2 FCR 82 at 88 (Bowen CJ, Lockhart and Fitzgerald JJ); *James v Australia and New Zealand Banking Group Ltd* (1986) 64 ALR 347 at 372 (Toohey J); *Wright v Wheeler Grace & Pierucci Pty Ltd* (1988) ATPR ¶40-865 at 49,375-49,376 (French J); affirmed in *Wheeler Grace & Pierucci Pty Ltd v Wright* (1989) 16 IPR 189; *Bateman v Slayter* (1987) 71 ALR 553 at 559 (Burchett J); and *Thompson v Ice Creameries of Australia Pty Ltd* (1998) ATPR ¶41-611 at 40,693 (Lehane J). Cf *Forrest v ASIC* (2012) 247 CLR 486, 525 [103] (Heydon J).
[144] *Rhone-Poulenc Agrochimie SA v UIM Chemical Services Pty Ltd* (1986) 12 FCR 477.

Assuming that the definition of 'conduct' in s 2 of the ACL can be satisfied, it is then necessary to consider whether silence at issue in a particular case was misleading in accordance with the reasonable expectations test considered in *Miller & Associates Insurance Broking Pty Ltd v BMW Australia Finance Limited*.[145] In that case French CJ and Kiefel J observed:

> Reasonable expectation analysis is unnecessary in the case of a false representation where the undisclosed fact is the falsity of the representation. A party to precontractual negotiations who provides to another party a document containing a false representation which is not disclaimed will, in all probability, have engaged in misleading or deceptive conduct. When a document contains a statement that is true, non-disclosure of an important qualifying fact will be misleading or deceptive if the recipient would be misled, absent such disclosure, into believing that the statement was complete.[146]

The 'reasonable expectation' test is predicated on the assumption that one party is aware of an undisclosed fact and the circumstances and context of the case give rise to an objectively reasonable expectation on the part of the other party that the fact should be disclosed because it would be relevant or material in its decision-making. The reasonableness of the alleged expectation is to be assessed objectively, and not by reference to the subjective expectation of the other party to the transaction.[147]
If the facts in the matter of *Sears Holdings Management Corporations* were to arise in Australia they may give rise to contraventions of ss 18 and /or 29(1)(g) of the ACL, or ss 12DA and/or 12DB(1) of the ASIC Act. Sears' initial communications failed to disclose adequately the extent of information that the software application would collect when installed. In an Australian context, the scope of the tracking would be material to consumers in deciding whether to consent to the installation of the software and give rise to an objectively reasonable expectation of full disclosure on the part of consumers prior to installation.

C Unconscionable Conduct

The second general protection of the ACL which may catch online privacy and data security breaches is contained in s 21(1) which provides that:

> A person must not, in trade or commerce, in connection with:
>
> (a) the supply or possible supply of goods or services to a person (other than a listed public company); or
>
> (b) the acquisition or possible acquisition of goods or services from a person (other than a listed public company);
>
> engage in conduct that is, in all the circumstances, unconscionable.

Section 21(1) is designed to protect persons generally, including 'business consumers' and 'business suppliers' from unconscionable conduct by persons occupying more powerful positions. There are no limits on the kind of businesses that might seek to rely on s 21(1); the only limitations are that the goods or services supplied or acquired must be supplied or acquired for the purpose of trade or commerce and the conduct must not be directed towards a publicly listed company.

In *Paciocco v Australia and New Zealand Banking Group*, the Court had to decide whether the late payment fee charged the ANZ bank on credit card accounts was a penalty or otherwise unconscionable for the purposes of the prohibition of statutory unconscionable conduct in s 12CB of the ASIC Act. The Full Federal Court held that the charging of the late payment fees by ANZ was not

[145] *Miller & Associates Insurance Broking Pty Ltd v BMW Australia Finance Limited* (2010) 241 CLR 357.
[146] Ibid at [23].
[147] Ibid at [20].

unconscionable. Allsop CJ said:

> More specific guidance to the meaning and operation of s 12CB as a consumer provision is given by the matters set out in s 12CC …to which a court may have regard for the purposes of considering the question of unconscionable conduct. These matters assist in setting a framework for the values that lie behind the notion of the relevant conscience of the parties in trade or commerce identified in s 12CB. Those values and conceptions can be seen as: fairness and equality: see paras (a), (b), (d) – (k); a lack of understanding or ignorance of a party: para (c); the risk and worth of the bargain: paras (e) and (i); and good faith and fair dealing: para (l).[148]

Allsop CJ stated that in applying s 12CB of the ASIC Act, what is required is:

> …an evaluation of business behaviour (conduct in trade or commerce) as to whether it warrants the characterisation of unconscionable, in the light of the values and norms recognised by the statute. The task is not limited to finding "moral obloquy"; such may only divert the normative inquiry from that required by the statute, to another, not tied to the words of the statute. [149]

Allsop CJ concluded:

> In all the circumstances, in particular, the lack of any proven predation on the weak or poor, the lack of real vulnerability requiring protection, the lack of financial or personal compulsion or pressure to enter or maintain accounts, the clarity of disclosure, the lack of secrecy, trickery or dishonesty, and the ability of people to avoid the fees or terminate the accounts, I do not consider the conduct of ANZ to have been unconscionable. To do so would require the court to be a price regulator in banking business in connection with otherwise honestly carried on business in which high fees were extracted from customers.[150]

The High Court was unanimous in dismissing the appeal that the Full Federal Court erred in determining that the charging of the late payment fees by ANZ was not unconscionable.[151] Two members of the High Court, Keane J and Gageler J, discussed statutory unconscionability. They did not depart from the analysis of Allsop CJ.

Keane J (with whom French CJ and Kiefel J agreed) gave the following reasons. First, late payment fees on credit cards were an established practice by all participants in the market, and the appellants had not argued that '…the market itself is unlawfully skewed'.[152] Secondly, there was no suggestion that Mr Paciocco was forced to incur the late payment fees as a result of poverty or financial difficulties. Rather, '…Mr Paciocco chose to pay late, and thereby incur the late payment fee, as a matter of his own convenience'.[153] Thirdly, the existence of a disparity in bargaining power alone is not enough to attract the operation statutory unconscionability. Rather, attention must focus on the manner of its exercise.[154]

[148] *Paciocco v Australia and New Zealand Banking Group* [2015] FCAFC 50 at [285].
[149] Ibid at [304]-[305].
[150] *Paciocco v Australia and New Zealand Banking Group* (2015) 236 FCR 199 at 283 [347].
[151] *Paciocco v Australia and New Zealand Banking Group* [2016] HCA 28.
[152] Ibid at [290].
[153] Ibid at [290].
[154] Ibid at [293] and [294].

Gageler J adopted the view that statutory unconscionable conduct is to be determined objectively and requires a 'high level of moral obloquy' on the part of the person said to have acted unconscionably.[155] His Honour concluded:

> The existence and amount of the late payment fee were disclosed to Mr Paciocco in the letters, booklets and telephone calls which he received from ANZ. He was able to, and did, understand them. There has never been any suggestion of undue influence or pressure having been exerted on him or of unfair tactics having been used against him. Mr Paciocco freely chose to enter into the two credit card contracts with ANZ and could have terminated those contracts at any time at will. He could at any time have sought to obtain a credit card from another bank. Other banks were in fact charging broadly equivalent fees. Mr Paciocco chose instead to maintain his accounts with ANZ, to manage those accounts at close to their limits and to bear the risk of being charged the late payment fee on those occasions when he failed to comply with the standard stipulation to make the minimum monthly payment by the due date.[156]

Obtaining Personal Information without Consent

If the facts in the matter of *Sears Holdings Management Corporations* were to arise in Australia they could give rise to a contravention of s 21 of the ACL. A number of the statutory factors in s 22(1) of the ACL may be taken in to account by the Court. First, in relation to s 22(1)(a) – the relative strengths of the bargaining positions of the supplier and the customer – the customer whose personal information is being collected is likely to be in a weak and vulnerable position arising from the information asymmetry as between the corporation and the customer. Secondly, in relation to s 22(1)(i) – the extent to which the supplier unreasonably failed to disclose to the customer any intended conduct of the supplier that might affect the interests of the customer – if the corporation requires consumers to download a software application that tracks their online behaviour and internet traffic, and the corporation fails to disclose that it on-sells that information to third party data brokers, this may constitute statutory unconscionable conduct. Arguably, the conduct would be contrary to fair dealing and conscience, and would involve a degree of moral tainting as a form of dishonest trickery or sharp practice.

D Unfair Terms

The third general protection relates to unfair terms in standard form consumer contracts and small business contracts. These are regulated by Part 2-3 of the ACL. The principal operative provisions relating to unfair terms are s 23(1) and (2) of the ACL which provide:

> (1) A term of a consumer contract or small business contract is void if:
>
> (a) the term is unfair; and
>
> (b) the contract is a standard form contract.
>
> (2) The contract continues to bind the parties if it is capable of operating without the unfair term.

The supply is not required to be from a person "in trade or commerce". However, the contract must be a standard form consumer or small business contract that contains an unfair term.

---

[155] Ibid at [188] applying *Attorney-General (NSW) v World Best Holdings Ltd* (2005) 63 NSWLR 557 at 583 [121] (Spigelman CJ); *CIT Credit Pty Ltd v Keable* [2006] NSWCA 130 (Spigelman CJ, with whom Giles JA and Gzell J agreed).
[156] Ibid at [190]

The test of what is "unfair" falls into four parts. The Court must consider the term at issue itself;[157] contextual matters surrounding the formation of the contract containing the term;[158] whether the term was transparent;[159] and the term at issue in the context of the contract as a whole.[160] In determining whether each of the elements of unfairness is satisfied, the Court obtains guidance from the indicative "grey" list in s 25 of the ACL. Section 25 provides non-exhaustive examples of the kinds of terms that may, depending on the particular circumstances, be unfair. The purpose of the grey list is to provide statutory guidance as to the terms that may be of concern; it does not create a presumption that those terms are unfair.

Section 25(g) provides the following example of a term which may be unfair:

> a term that permits, or has the effect of permitting, one party unilaterally to vary the characteristics of the goods or services to be supplied, or the interest in land to be sold or granted, under the contract.

An example of such a term in the context of privacy and data security breaches is one that allows for retroactive changes to privacy policies.

Another example of a potentially unfair term is one that "limits, or has the effect of limiting, one party's right to sue another".[161] Such a term may attempt to compel the consumer to have any dispute arising from a privacy or data security breach decided by a private arbitrator, or expressly prohibit the consumer from participating in a class action.

VI PRIVATE AND PUBLIC REMEDIES UNDER THE ACL FOR MISLEADING PRIVACY AND DATA SECURITY CLAIMS

A contravention of the consumer protection provisions in the ACL can be pursued in two ways. First, by means of private enforcement by persons who have suffered loss or damage caused by the conduct that contravenes the ACL; and secondly, by means of public enforcement by the ACCC.

A Private Actions

[157] ACL, s 24(1).
[158] ACL, s 24(2).
[159] ACL, s 24(2)(a).
[160] ACL, s 24(2)(b).
[161] ACL, s 25(k).

Consumers who suffer loss or damage as a result of the misleading privacy and data security claims may bring private actions for damages,[162] compensation orders,[163] and/or an injunction.[164] If consumers become aware of breaches they may not have a sufficient incentive to bring private actions. There are a number of reasons why an individual consumer may not have a sufficient incentive to bring a private action. First, as explained in Part V above, the application of the ACL to online privacy or data security breaches is not clear-cut in some circumstances. Secondly, in private actions for damages the onus is on the consumer to prove a breach of the ACL on the balance of probabilities. The adversarial nature of the legal system provides little incentive for an individual consumer to take on the might of a large corporation that is prepared to devote significant financial resources to defend the action. If the consumer is successful on the issue of liability, the consumer must quantify the loss or damage suffered. Damages are not easy to measure for a breach of privacy. Are damages available for anxiety or stress in an action for a contravention of ss 18 or 21 of the ACL? Finally, the consumer must prove individual reliance on the misleading or unconscionable conduct of the respondent. Section 236 of the ACL only entitles a consumer to damages if the consumer can prove by objective evidence, rather than self-serving assertion, that the consumer relied on the misleading or unconscionable conduct of the respondent.[165] This may prove difficult in practice.

Where the loss or damage was partly the fault of the consumer in failing to take reasonable care, s 137B of the CCA provides for a contributory fault defence for damages under s 236 of the ACL. There are also proportionate liability provisions in Pt VIA of the CCA that apply in respect of a claim for damages under s 236 of the ACL. Section 87CD(1)(a) of the CCA requires the Court to apportion the liability of a defendant who is a "concurrent wrongdoer",[166] on the basis of what it considers "just" having regard to the extent of the defendant's responsibility for the damage or loss. Thus, in the case of loss or damage arising from computer hacking, there would be a prospect of apportionment to the primary wrongdoer (the hacker), which would reduce the loss or damage payable by the corporation storing the consumer's personal data that was hacked. Finally, there are many practical difficulties with bringing private actions by consumers, not the least of which is the high cost of legal services and the risk of having to pay the defendant's legal costs as well if the consumer is unsuccessful.

One way of overcoming these difficulties is for a consumer, or group of consumers affected by a data breach, to obtain funding from a litigation funding company. Such companies provide funds and manage disputes on behalf of their clients in return for a share of the damages awarded. They also agree to pay the costs of the defendant in the event of an adverse costs order.

Class actions may be another means of overcoming these practical difficulties. The class action is a device for offsetting the high cost of legal services. If numerous consumers suffer the same injury as a result of a privacy breach or data security breach, but the loss or damage suffered by each of them is not sufficient to justify bringing separate proceedings, one or more may bring proceedings on behalf of the entire class of injured consumers. For example, representative proceedings can be brought under Pt IVA of the *Federal Court of Australia Act 1976* (Cth) (FCA).[167] Section 33C(1) of the FCA allows a representative proceeding to be commenced where the claims of the persons who are proposed as members of a group arose out of "the same, similar or related circumstances". Pt IVA

[162] ACL, s 236.
[163] ACL, s 237.
[164] ACL, s 232.
[165] See *Access to Justice Arrangements*, Productivity Commission Inquiry Report No. 72, 5 September 2014 which identifies a range of access to justice problems under Australia's civil justice system.
[166] This is defined in s 87CB(3) of the CCA as one of two or more persons whose "acts or omissions (or act or omission) caused, independently of each other or jointly, the damage or loss that is the subject of the claim". It is irrelevant that a wrongdoer is insolvent, being wound up or has ceased to exist or died. This has the potential to disadvantage consumers where one or more of the wrongdoers is insolvent or has ceased to exist.
[167] The history and purposes of Pt IVA are described by French J in *Zhang de Yong v Milgea* (1993) 118 ALR 165 at 183. See Damian Grave, Ken Adams and Jason Betts, *Class Actions in Australia* (2nd ed, Lawbook Co,, Sydney, 2012).

proceeds on the basis that the consent of a person to be a member of the group is not required.[168] The Court must fix a date before which a group member may opt out of a representative proceeding.[169] Section 33Z of the FCA provides that the Court may in a representative proceeding determine issues of law and fact; make a declaration of liability; grant any equitable relief; make an award of damages for group members; and make such other order as the Court thinks just.

B. Public Enforcement

In addition to private enforcement the ACL provides for public enforcement by the ACCC. This can be in the form of civil sanctions in relation to the contraventions of one or more the provisions of Chs 2 or 3 of the ACL (other than s 18), or the imposition of criminal sanctions in relation to the offences contained in Ch 4 of the ACL. The civil prohibitions in ss 29(1)(a) and (g) and s 33 of the ACL are replicated in Chapter 4 of the ACL as criminal offences. Section 151 replicates s 29(1) and s 155 replicates s 33. The ACCC has a broad authority to enforce the civil prohibitions and criminal offences in the ACL. The ACCC has two discretionary administrative powers which may be used in relation to privacy and data security claims, substantiation notices and infringement notices.

Substantiation Notices

Substantiation notices are likely to be used by the ACCC in relation to misleading privacy and data security claims where the ACCC cannot readily discern the truth or accuracy of the claim being made. A substantiation notice must be complied with within 21 days of the notice. Providing false or misleading information in a substantiation notice gives rise to civil and criminal liability. Section 222(1) provides that a person must not provide the regulator false or misleading information in compliance or purported compliance with a substantiation notice.

Part 4-5 of the ACL sets out criminal offence provisions for failing to comply with a substantiation notice. Penalties for failing to comply with it within the substantiation notice compliance period are $16,500 for a body corporate, and $3,300 for a person who is not a body corporate. The ACCC also has extensive evidence gathering powers pursuant to s 155 of the CCA. For example, in the course of its investigation in *ACCC v Safe Breast Imaging Pty Ltd*,[170] the company was required pursuant to s 155 to provide details of the published clinical trials and scientific research into the efficacy of the MEM device for breast imaging in order to establish whether there was a reasonable scientific basis supporting the representations made.[171]

Infringement Notices

Infringement notices may be issued by the ACCC where it has formed the view that a person has contravened ss 29(1) and/ or 33 of the ACL. The ACCC is not required to give the company a written statement that sets out ACCC's reasons for believing that a contravention has occurred; or give a representative of the company an opportunity to make submissions, give evidence and appear at a private hearing before the ACCC; or detail the circumstances giving rise to ACCC's reasons to believe a contravention has occurred. A failure to pay an infringement notice penalty may result in the ACCC commencing proceedings for the imposition of a criminal sanction or civil penalty.[172]

Infringement notices cannot be issued for an alleged contravention of s 18 of the ACL, the general misleading or deceptive conduct provision, possibly for the same reason that pecuniary penalties cannot be imposed for a contravention of s 18.[173] Because of its general nature it may involve breaches of the law that are unintentional and inadvertent, and it would be inappropriate to penalise

[168] FCA, s33E.
[169] FCA, s33J.
[170] *ACCC v Safe Breast Imaging Pty Ltd* (2014) ATPR ¶42-464.
[171] Ibid at [135].
[172] See ACCC, *Guidelines on the Use of Infringement Notices* (issued on 16 October 2012) at [9].
[173] CCA, s 134A(2).

such conduct. If the ACCC has reasonable grounds for believing that a person has contravened an infringement notice provision within 12 months after the day on which the contravention is alleged to have occurred, the ACCC may issue an infringement notice. If the penalty is paid, the matter is closed without proceeding to court.

Section 134(1) of the CCA provides that the issue of an infringement notice to a person for an alleged contravention is "… as an alternative to proceedings for an order under section 224 of the Australian Consumer Law". Thus, the ACCC cannot issue an infringement notice and subsequently seek pecuniary penalties in relation to the same alleged contravention. Infringement notices carry penalties of $102,000 for ASX-listed corporations, $10,200 for bodies corporate other than listed corporations and $2,040 for individuals. [174]

Civil and Criminal Proceedings

In more serious cases of misleading privacy and data security claims the ACCC may apply to the Court for the imposition of civil or criminal sanctions. The maximum civil pecuniary penalties that can be imposed for *each* contravention of the specific consumer protections provisions (not the general protection in s 18 of the ACL) are $1.1 million for a body corporate and $220,000 for persons other than bodies corporate.[175] The matters to be taken into account by the Court in assessing an appropriate penalty are set out in s 224(2) of the ACL. Where natural persons are knowingly concerned in making false premium claims the ACCC will seek to make them liable as accessories pursuant to s 224(1)(e) of the ACL.

In addition to pecuniary penalties, the Court can order any of the following:

- declarations;[176]
- injunctions to prevent the prohibited conduct from continuing or being repeated;[177]
- non-punitive relief for non-party consumers;[178]
- non-punitive relief orders, such as for the establishment of a compliance program and an order to publish corrective advertising to protect the public interest;[179]
- orders disqualifying persons from managing a corporation for breaches of the specific consumer protection provisions;[180] and
- Court enforceable undertakings.[181]

The ACCC cannot pursue all of the complaints it receives and must direct its enforcement resources to ensuring it obtains the greatest overall benefit for consumers.[182] To date the ACCC has not sought to bring civil or criminal proceedings for online privacy or data security breaches. This may be because it has not received any complaints of that nature, or that, unlike the FTC, it gives these types of breaches very little priority. The enforcement of privacy rights in Australia is at a very early stage of its development, and given all of its other priorities, the ACCC may feel that these matters should be left to the specialist regulator in this area, the OAIC, or industry regulators such as the Australian Energy Regulator, which issued an infringement penalty in June 2014 against Lumo Energy for its failure to meet information security standards in breach of the National Electricity Rules.[183]

---

[174] CCA s 134C.
[175] ACL, s 224.
[176] Pursuant to s 21 of the *Federal Court of Australia Act 1976* (Cth).
[177] ACL, s 232.
[178] ACL 239(1).
[179] ACL s 246(1).
[180] ACL, s 248.
[181] CCA, s87B.
[182] See Australian Consumer Law, *Compliance and Enforcement, How Regulators Enforce the Australian Consumer Law*, 7.
[183] Jackson and Hughes, above n 25, 140.

However, claims made by corporations, especially those operating in an online environment, about the safe storage of data, and measures to ensure the protection of consumers' confidential information are in the nature of premium claims. Premium claims have been an enforcement priority for the ACCC since 2013.[184] Premium claims give the impression that a product or service has attributes, or some kind of added benefit when compared to similar products and services. They can be made as long as the claims are not misleading and can be substantiated.[185] False premium claims about privacy protection and data security will difficult, or impossible for consumers to detect because of information asymmetries. By providing both public and private avenues of enforcement, the ACL has the potential to serve as a useful instrument in regulating online privacy and data security breaches against consumer.

VII. CONCLUSION

The issue of online privacy and data security is very important for businesses and Australian society in general. The amount of consumers' personal data that is being collected from websites is increasing exponentially. However, very little is known about the extent to which corporations in Australia are collecting data on their customers' transactions and spending patterns, and the extent to which this data is being shared with others. Australia lags behind comparable developed countries in relation to data protection. International frameworks, such as the OECD Guidelines, have been in place since 1980. In Australia, the *Privacy Act 1988* (Cth), imposes some limited obligations and protections for consumers. It provides for penalties, but these penalties only apply to serious or repeated invasions of privacy. As digital practices such as data sharing and ecommerce becoming increasingly commonplace, it is imperative that Australia develop a strong legal framework for regulating cyber security. While the setting out specific legal obligations for businesses by way of the *Privacy Act* is an appropriate regulatory response to the problem of protecting privacy and data security, the broad, general protections of the *Australian Consumer Law* and *ASIC Act* also have a role to play in this area. Consumer protection laws seek to ensure that consumers make an informed choice when entering into particular transactions. They seek to ensure that consumer reasonable expectations regarding privacy and data security are met. Finally, they offer effective remedies in relation to privacy violations.

[184] See *ACCC Compliance and Enforcement Policy* (February 2015), p 4.
[185] ACCC, *False or misleading claims*. Available at: http://www.accc.gov.au/business/advertising-promoting-your-business/false-or-misleading-statements